

**APPEAL BRIEF UNDER 37 C.F.R. § 41.37**

**TABLE OF CONTENTS**

	<u>Page</u>
<b><u>1. REAL PARTY IN INTEREST</u></b> .....	2
<b><u>2. RELATED APPEALS AND INTERFERENCES</u></b> .....	3
<b><u>3. STATUS OF THE CLAIMS</u></b> .....	4
<b><u>4. STATUS OF AMENDMENTS</u></b> .....	5
<b><u>5. SUMMARY OF CLAIMED SUBJECT MATTER</u></b> .....	6
<b><u>6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL</u></b> .....	10
<b><u>7. ARGUMENT</u></b> .....	11
<b><u>8. SUMMARY</u></b> .....	16
<b><u>CLAIMS APPENDIX</u></b> .....	17
<b><u>EVIDENCE APPENDIX</u></b> .....	24
<b><u>RELATED PROCEEDINGS APPENDIX</u></b> .....	25

S/N 10/750,529

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant:	Kevin R. Driscoll	Examiner: Fikremariam Yalew
Serial No.:	10/750,529	Group Art Unit: 2136
Filed:	December 31, 2003	Docket No.: H0005071.35998
Title:	DATA AUTHENTICATION AND TAMPER DETECTION	

---

**APPEAL BRIEF UNDER 37 CFR § 41.37**

Mail Stop Appeal Brief- Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

The Appeal Brief is presented in response to the rejection of claims 1-35 of the above-identified application, as set forth in the Notice of Panel Decision from Pre-Appeal Brief mailed February 26, 2009.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of \$540.00 which represents the requisite fee set forth in 37 C.F.R. § 41.20(b)(2). The Appellants respectfully request consideration and reversal of the Examiner's rejections of pending claims.

**1. REAL PARTY IN INTEREST**

The real party in interest of the above-captioned patent application is the assignee, Honeywell International Inc.

## **2. RELATED APPEALS AND INTERFERENCES**

There are no other appeals or interferences known to Appellant that will have a bearing on the Board's decision in the present appeal.

### **3. STATUS OF THE CLAIMS**

The present application was filed on December 31, 2003 with 35 claims. In response to the Office Action mailed December 28, 2006, an Amendment was filed to amend claims 1, 4, 9, 13 and 24-35. In response to the Final Office Action mailed July 10, 2008, an Amendment was filed to amend claims 1, 5, 13, 24 and 28. Claims 1-35 are subject of the present Appeal.

#### **4. STATUS OF AMENDMENTS**

No amendments have been made subsequent to the Final Office Action mailed November 4, 2008.

## **5. SUMMARY OF CLAIMED SUBJECT MATTER**

Some aspects of the present inventive subject matter include, but are not limited to, methods, systems and apparatus for data authentication and tamper detection. In claim 1, a method includes receiving an ephemeral value from a challenging device. See FIG. 1 – challenge device 102, FIG. 6 – block 602 and Application at ¶0047. The method includes retrieving data whose content is known to the challenging device. See FIG. 1 – challenge device 102, FIG. 6 – block 604 and Application at ¶0048. The method also includes performing data authentication, wherein performing the data authentication comprises generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value. See FIG. 6 – block 606 and Application at ¶0049-0050. The method includes transmitting the digital signature to the challenging device. See FIG. 1 – challenge device 102, FIG. 6 – block 608 and Application at ¶0051.

In claim 5, a method includes receiving, into a response device, an ephemeral value from a challenge device. See FIG. 1 – challenge device 102 and response device 104, FIG. 6 – block 602 and Application at ¶0047. The method includes retrieving data from an address space in the response device, wherein the data is known to the challenge device and the response device. See FIG. 1 – challenge device 102 and response device 104, FIG. 6 – block 604 and Application at ¶0048. The method also includes performing data authentication of data stored in the challenge device, wherein performing the data authentication comprises generating a hash across the data using the ephemeral value as a key of the hash. See FIG. 6 – block 606 and Application at ¶0049-0050. The method includes transmitting at least part of the hash to the challenge device. See FIG. 1 – challenge device 102, FIG. 6 – block 608 and Application at ¶0051.

In claim 9, a method includes authenticating data having predictable content and stored in an address space of a remote device. See FIG. 1 – challenge device 102, FIG. 5 – flow diagram 500 and Application at ¶0036-0045. The authenticating includes generating a random number. See FIG. 5 – block 502 and Application at ¶0037. The authenticating includes transmitting the random number to a remote device presumably

having the data. See FIG. 5 – blocks 504-506 and Application at ¶0038-0039. The authenticating includes receiving, from the remote device, a first digital signature that is representative of the data. See FIG. 1 – challenge device 102, FIG. 5 – block 508 and Application at ¶0040. The authenticating includes generating a second digital signature with a cryptographic key having a value that is equal to the random number. See FIG. 5 – blocks 510 and Application at ¶0041. The authenticating also includes comparing the first digital signature to the second digital signature. See FIG. 5 – blocks 512 and Application at ¶0042.

In claim 13, an apparatus includes a storage medium to store data. See FIG. 3 – storage medium 308 and Application at ¶0028. The apparatus also includes an input/output (I/O) logic to receive a request for authentication from a challenge device, wherein the request includes an ephemeral value. See FIG. 3 – I/O logic 304 and Application at ¶0028 and 0047. The apparatus also includes a signature logic to retrieve at least part of the data from the storage medium and to perform data authentication of the data, wherein the data authentication comprises generation of a cryptographic hash across the at least part of the data with a cryptographic key having a value that is equal to the ephemeral value. See FIG. 3 – signature logic 302 and Application at ¶0029 and 0049-0050.

In claim 20, a challenge device to authenticate data presumably stored in a response device includes a storage medium to store a copy of the data presumed to be stored in the response device. See FIG. 2 – challenge device 102 and storage medium 210 and Application at ¶0024-0025. The challenge device also includes a key generation logic to generate an ephemeral value. See FIG. 2 – key generation logic 202 and Application at ¶0026 and 0037. The challenge device includes an input/output (I/O) logic to output a request for authentication to a response device, wherein the request includes the ephemeral value, the I/O logic to receive a first digital signature from the response device in response to the request for authentication. See FIG. 2 – I/O logic 206 and Application at ¶0026 and 0038-0039. The challenge device includes a signature logic to retrieve the copy of the data and the ephemeral value and to generate a second digital signature. See FIG. 2 – signature logic 204 and Application at ¶0026 and 0041. The



challenge device also includes an authentication logic to compare the first digital signature to the second digital signature, wherein the data is authenticated if the first digital signature equals the second digital signature. See FIG. 2 – signature logic 212 and Application at ¶0026 and 0042.

In claim 24, a physical machine-readable medium provides instructions, which when executed by a machine, cause said machine to perform operations. See machine-readable medium in computer system 400 and Application at ¶0034. The operations include receiving an ephemeral value from a challenging device. See FIG. 1 – challenge device 102, FIG. 6 – block 602 and Application at ¶0047. The operations include retrieving data whose content is known to the challenging device. See FIG. 1 – challenge device 102, FIG. 6 – block 604 and Application at ¶0048. The operations include performing data authentication, wherein performing the data authentication comprises generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value. See FIG. 6 – block 606 and Application at ¶0049-0050. The operations include transmitting the digital signature to the challenging device. See FIG. 1 – challenge device 102, FIG. 6 – block 608 and Application at ¶0051.

In claim 28, a physical machine-readable medium provides instructions, which when executed by a machine, cause said machine to perform operations. See machine-readable medium in computer system 400 and Application at ¶0034. The operations include receiving, into a response device, an ephemeral value from a challenge device. See FIG. 1 – challenge device 102 and response device 104, FIG. 6 – block 602 and Application at ¶0047. The operations include retrieving data from an address space in the response device, wherein the data is known to the challenge device and the response device. See FIG. 1 – challenge device 102 and response device 104, FIG. 6 – block 604 and Application at ¶0048. The operations include performing data authentication of data stored in the challenge device, wherein performing the data authentication comprises

generating a hash across the data using the ephemeral value as a key of the hash. See FIG. 6 – block 606 and Application at ¶0049-0050. The operations include transmitting at least part of the hash to the challenge device. See FIG. 1 – challenge device 102, FIG. 6 – block 608 and Application at ¶0051.

In claim 32, a physical machine-readable medium provides instructions, which when executed by a machine, cause said machine to perform operations. See machine-readable medium in computer system 400 and Application at ¶0034. The operations include authenticating data having predictable content and stored in an address space of a remote device. See FIG. 1 – challenge device 102, FIG. 5 – flow diagram 500 and Application at ¶0036-0045. The authenticating includes generating a random number. See FIG. 5 – block 502 and Application at ¶0037. The authenticating includes transmitting the random number to a remote device presumably having the data. See FIG. 5 – blocks 504-506 and Application at ¶0038-0039. The authenticating includes receiving, from the remote device, a first digital signature that is representative of the data. See FIG. 1 – challenge device 102, FIG. 5 – block 508 and Application at ¶0040. The authenticating includes generating a second digital signature with a cryptographic key having a value that is equal to the random number. See FIG. 5 – blocks 510 and Application at ¶0041. The authenticating also includes comparing the first digital signature to the second digital signature. See FIG. 5 – blocks 512 and Application at ¶0042.

This summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellant refers to the appended claims and its legal equivalents for a complete statement of the invention.

**6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Claims 1-8 and 13-31 were rejected under 35 U.S.C. § 102(e) for anticipation by Grawrock et al. (hereinafter referred to as Grawrock) U.S. Patent No. 2002/0080974 B2. Claims 9-12 and 32-35 were rejected under 35 USC § 103(a) as being unpatentable over Johnson, P.K. et al. (hereinafter referred to as Johnson) (WO 00/18162) in view of Grawrock.

## **7. ARGUMENT**

### **A) The Applicable Law for Rejection under 35 U.S.C. § 102**

Anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration. *In re Dillon* 919 F.2d 688, 16 USPQ 2d 1897, 1908 (Fed. Cir. 1990) (en banc), cert. denied, 500 U.S. 904 (1991). It is not enough, however, that the prior art reference discloses all the claimed elements in isolation. Rather, “[a]nticipation requires the presence in a single prior reference disclosure of each and every element of the claimed invention, *arranged as in the claim.*” *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 221 USPQ 481, 485 (Fed. Cir. 1984) (citing *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 220 USPQ 193 (Fed. Cir. 1983)) (emphasis added). “The identical invention must be shown in as complete detail as is contained in the ... claim.” *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989); MPEP § 2131.

### **B) Discussion of the rejection of claims 1-8 and 13-31 were rejected under 35 U.S.C. § 102(e) for anticipation by Grawrock**

Applicant respectfully traverses. Among the differences, claim 1 recites “performing data authentication, wherein performing the data authentication comprises generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value.” Claim 13 includes a similar limitation.

In the Response to Arguments section??, the Office indicated that Grawrock teaches generating a digital signature based on an ephemeral value at 0028-0029, 0034 and steps 310, 315 in Fig. 3. Applicant respectfully traverses. Grawrock at 0028-0029 relates to a digital signature. However, this digital signature is not signed with a key that is equal to an ephemeral value. In contrast, this digital signature is signed “with a private key (CAPRK) of a certification authority . . .” Grawrock at [0028]. In Grawrock, the

CAPRK is not defined as an ephemeral value. Rather, the EUPUK and the EAPRK are keys that are equal to an ephemeral value. Grawrock at 0034 relates to performing a hash operation “on the EAPUK. . .”, not using the EAPUK to perform the hash. In other words, the EAPUK is data that is being hashed. Grawrock at steps 310 and 315 of Fig. 3 relate generally to ephemeral keys (EAPUK and EAPRK). However, this section of Grawrock does not disclose generating a digital signature using a key that has a value equal to an ephemeral value.

Further, the Office alleges that performing encryption is equivalent to generating a digital signature or hash:

Further more the system in Grawrok (sic) relates to use of ephemeral value as a cryptographic key to perform encryption/decryption of data(i.e., the examiner reasonably interpreted using ephemeral value as a cryptographic key to perform encryption equivalent to use of an ephemeral value as a cryptographic key generate a digital signature or hash).

Office Action at page 2.

Applicant respectfully traverses. Encryption does not equal digital signature generation. Encryption is a reversible operation used to protect the data. Digital signature generation is used to authenticate the data. Protection does not equal authentication (as recited in claims 1, 5, 13, 24 and 28). For example, among the differences, claim 1 recites “performing data authentication, wherein performing the data authentication comprises generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value.” (emphasis added).

Further, in the Response to Arguments section, the Office indicated that Grawrock teaches performing data authentication at steps 325 and 330 of Fig. 3 (regarding the description of “validate identify using identify credential.”). Office Action at page 3. In Grawrock, the identity credential relates to “(i) secret data associated with the identity (e.g., a permanent asymmetric public key of the identity, referred to as the “identity public key”) and (ii) a first sequence of alphanumeric characters (e.g., a statement “TCPA Subsystem Identity”).” Grawrock at [0028]. This credential is “digitally signed with a private key (CAPRK).” As noted above, in Grawrock, the

CAPRK is not defined as an ephemeral value. Rather, the EUPUK and the EAPRK are keys that are equal to an ephemeral value. Therefore, Grawrock does not disclose data authentication comprising generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value.

Because Grawrock does not disclose all of the claim limitations, Applicant respectfully submits that the rejection of claims 1, 5, 13, 24 and 28 under 35 USC § 102 has been overcome. Because claims 2-4, 6-8, 14-19, 25-27 and 29-31 depend from and further define claims 1, 5, 13, 24 and 28, respectively, Applicant respectfully submits that the rejection of claims 2-4, 6-8, 14-19, 25-27 and 29-31 under 35 USC § 102 has been overcome.

### **C) The Applicable Law for Rejection under 35 U.S.C. § 103**

The Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d (BNA) 1596, 1598 (Fed. Cir. 1988). As discussed in *KSR International Co. v. Teleflex Inc. et al.* (U.S. 2007), the determination of obviousness under 35 U.S.C. § 103 is a legal conclusion based on factual evidence. *See Princeton Biochemicals, Inc. v. Beckman Coulter, Inc.*, 7, 1336-37 (Fed. Cir. 2005). The legal conclusion, that a claim is obvious within § 103(a), depends on at least four underlying factual issues set forth in *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17 (1966): (1) the scope and content of the prior art; (2) differences between the prior art and the claims at issue; (3) the level of ordinary skill in the pertinent art; and (4) evaluation of any relevant secondary considerations.

The *KSR* Court further held that “rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” (*See In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006) cited with approval in *KSR Int'l v. Teleflex Inc.*, 127 S. Ct. 1727, 1740-41 (2007)).

Therefore, the test for obviousness under §103 must take into consideration the invention as a whole; that is, one must consider the particular problem solved by the

combination of elements that define the invention. (*Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir.1985).) The Examiner must, as one of the inquiries pertinent to any obviousness inquiry under 35 U.S.C. §103, recognize and consider not only the similarities but also the critical differences between the claimed invention and the prior art. (*In re Bond*, 910 F.2d 831,834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990), *reh'g denied*, 1990 U.S. App. LEXIS 19971 (Fed. Cir.1990).) Critical differences in the prior art must be recognized (when attempting to combine references). (*In re Bond*, 910 F.2d 831,834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990), *reh'g denied*, 1990 U.S. App. LEXIS 19971 (Fed. Cir.1990).)

Moreover, the fact that a reference teaches away from a claimed invention is highly probative that the reference would not have rendered the claimed invention obvious to one of ordinary skill in the art. (*Stranco Inc. v. Atlantes Chemical Systems, Inc.*, 15 USPQ2d 1704, 1713 (Tex. 1990).) When the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvious. (*Id.* at 4 citing *United States v. Adams*, 383 U.S. 39, 51-51 (1966).)

“If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious.” (*In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). The CCPA has also noted that “[t]he court must be ever alert not to read obviousness into an invention on the basis of the applicant’s own statements; that is, we must view the prior art without reading into that art appellant’s teachings.” *In re Sponnoble*, 160 USPQ 237, 243 (CCPA 1969). These principles have not been changed by the ruling in *KSR*.

**D) Discussion of the rejection of claims 9-12 and 32-35 were rejected under 35 USC § 103(a) as being unpatentable over Johnson in view of Grawrock.**

Applicant respectfully traverses. Neither Johnson nor Grawrock (alone or in combination) discloses or suggests all of the claim limitations.

Among the differences, claims 9 and 32 recite “generating a second digital signature with a cryptographic key having a value that is equal to the random number.” In the Response to Arguments section, the Office indicated that Grawrock teaches this limitation at 0033-0034 and Fig. 5 steps 530, 540. Applicant respectfully traverses. These section of Grawrock relate to performing a hash operation “on the EAPUK. . .”, not using the EAPUK to perform the hash. Further, Applicant respectfully submits that there is no suggestion to modify Grawrock to generate a digital signature. In contrast, in order to be operative, Grawrock requires encryption/decryption of the data using a cryptographic key having a value that is equal to a random number such that the data can be reproduced so that the static markers can be verified. In contrast, claims 9 and 32 recite the generating of a digital signature with such a cryptographic key. However, as noted above, the digital signature cannot be used to reproduce the encrypted data. Rather, the digital signature is used to authenticate.

Because neither Johnson nor Grawrock (alone or in combination) discloses or suggests all of the claim limitations, Applicant respectfully submits that the rejection of claims 9 and 32 under 35 USC § 103 has been overcome. Because claims 10-12 and 33-35 depend from and further define claims 9 and 32, respectively, Applicant respectfully submits that the rejection of claims 10-12 and 33-35 under 35 USC § 103 has been overcome.



## 8. SUMMARY


It is respectfully submitted that the claims are patentable over the cited art.  
Reversal of the rejection and allowance of the pending claim are respectfully requested.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.  
P.O. Box 2938  
Minneapolis, MN 55402  
(612) 371-2103

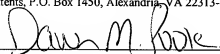
Date April 27, 2009

By

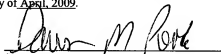
  
\_\_\_\_\_  
Gregg A. Peacock  
Reg. No. 45,001

**CERTIFICATE UNDER 37 CFR 1.8:** The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: MS Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 27th day of April, 2009.

Name

  
\_\_\_\_\_  
Dawn M. Rode

Signature

  
\_\_\_\_\_  
Dawn M. Rode

### **CLAIMS APPENDIX**

1. A method comprising:  
receiving an ephemeral value from a challenging device;  
retrieving data whose content is known to the challenging device;  
performing data authentication, wherein performing the data authentication comprises generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value; and  
transmitting the digital signature to the challenging device.
2. The method of claim 1, wherein receiving the ephemeral value from the challenging device comprises receiving a randomly generated number from the challenging device.
3. The method of claim 1, wherein retrieving the data comprises retrieving at least part of application code.
4. The method of claim 1, wherein generating the digital signature of the data based on the ephemeral value comprises generating a one-way hash across the data with the cryptographic key having a value that is equal to the ephemeral value.
5. A method comprising:  
receiving, into a response device, an ephemeral value from a challenge device;  
retrieving data from an address space in the response device, wherein the data is known to the challenge device and the response device;

performing data authentication of data stored in the challenge device, wherein performing the data authentication comprises generating a hash across the data using the ephemeral value as a key of the hash; and

transmitting at least part of the hash to the challenge device.

6. The method of claim 5, further comprising generating a reduced hash based on the hash, wherein transmitting the ephemeral value and the at least part of the hash to the challenge device comprises transmitting the ephemeral value and the reduced hash to the challenge device.

7. The method of claim 5, wherein retrieving the data from the address space in the response device comprises retrieving application code to be executed in the response device.

8. The method of claim 5, wherein retrieving the data from the address space in the response device comprises retrieving configuration parameters of the response device.

9. A method comprising:

authenticating data having predictable content and stored in an address space of a remote device, the authenticating comprising:

generating a random number;

transmitting the random number to a remote device presumably having the data;

receiving, from the remote device, a first digital signature that is representative of the data;

generating a second digital signature with a cryptographic key having a value that is equal to the random number; and  
comparing the first digital signature to the second digital signature.

10. The method of claim 9, wherein authenticating the data having predictable content comprises authenticating an application executable.

11. The method of claim 9, wherein authenticating the data having predictable content comprises authenticating at least one security parameter.

12. The method of claim 9, wherein authenticating further comprises marking the data as authenticated if the first digital signature equals the second digital signature.

13. An apparatus comprising:  
a storage medium to store data;  
an input/output (I/O) logic to receive a request for authentication from a challenge device, wherein the request includes an ephemeral value; and  
a signature logic to retrieve at least part of the data from the storage medium and to perform data authentication of the data, wherein the data authentication comprises generation of a cryptographic hash across the at least part of the data with a cryptographic key having a value that is equal to the ephemeral value.

14. The apparatus of claim 13, wherein the I/O logic is to receive the request for authentication from a challenge device, the I/O logic to transmit the cryptographic hash back to the challenge device.

15. The apparatus of claim 13, wherein the storage medium is a nonvolatile memory.

16. The apparatus of claim 13, further comprising a data selection logic to select less than all of the data, wherein the at least part of the data is the less than all of the data.

17. The apparatus of claim 16, wherein the data selection logic is to select less than all of the data based on a random number based selection of segments of the data.

18. The apparatus of claim 13, wherein the data comprises an application to be executed in the apparatus.

19. The apparatus of claim 13, wherein the data comprises at least one security parameter of the apparatus.

20. A challenge device to authenticate data presumably stored in a response device, the challenge device comprising:

a storage medium to store a copy of the data presumed to be stored in the response device;

a key generation logic to generate an ephemeral value;

an input/output (I/O) logic to output a request for authentication to a response device, wherein the request includes the ephemeral value, the I/O logic to receive a first digital signature from the response device in response to the request for authentication;

a signature logic to retrieve the copy of the data and the ephemeral value and to generate a second digital signature; and

an authentication logic to compare the first digital signature to the second digital signature, wherein the data is authenticated if the first digital signature equals the second digital signature.

21. The challenge device of claim 20, wherein the ephemeral value comprises a randomly generated value.
22. The challenge device of claim 20, wherein the data comprises application code to be executed by the response device.
23. The challenge device of claim 20, wherein the data comprises at least one configuration parameter of the remote device.
24. A physical machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:
  - receiving an ephemeral value from a challenging device;
  - retrieving data whose content is presumed known to the challenging device;
  - performing data authentication, wherein performing the data authentication comprises generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value; and
  - transmitting the digital signature to the device.
25. The physical machine-readable medium of claim 24, wherein receiving the ephemeral value from the device comprises receiving a randomly generated value from the device.

26. The physical machine-readable medium of claim 24, wherein retrieving the data comprises retrieving at least part of application code.

27. The physical machine-readable medium of claim 24, wherein generating the digital signature of the data based on the ephemeral value comprises generating a one-way hash across the data with the cryptographic key having a value that is equal to the ephemeral value.

28. A physical machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

receiving, into a response device, an ephemeral value from a challenge device;

retrieving data from an address space in the response device, wherein the data is presumed known to the challenge device;

performing data authentication of data stored in the challenge device, wherein performing the data authentication comprises generating a hash across the data using the ephemeral value as a key of the hash; and

transmitting at least part of the hash to the challenge device.

29. The physical machine-readable medium of claim 28, further comprising generating a reduced hash based on the hash, wherein transmitting the ephemeral value and the at least part of the hash to the challenge device comprises transmitting the ephemeral value and the reduced hash to the challenge device.

30. (Previously Presented) The physical machine-readable medium of claim 28, wherein retrieving the data from the address space in the response device comprises retrieving application code to be executed in the remote device.

31. (Previously Presented) The physical machine-readable medium of claim 28, wherein retrieving the data from the address space in the response device comprises retrieving configuration parameters of the remote device.

32. A physical machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

authenticating the data having predictable content and stored in an address space of a remote device, the authenticating comprising:

generating a random number;

transmitting the random number to a device presumably having the data;

receiving a first digital signature that is representative of the data;

generating a second digital signature with a cryptographic key having a value that is equal to the random number; and

comparing the first digital signature to the second digital signature.

33. The physical machine-readable medium of claim 32, wherein authenticating the data having predictable content comprises authenticating an application executable.

34. The physical machine-readable medium of claim 32, wherein authenticating the data having predictable content comprises authenticating at least one security parameter.

35. The physical machine-readable medium of claim 32, wherein authenticating further comprises marking the data as authenticated if the first digital signature equals the second digital signature.



**EVIDENCE APPENDIX**

None.

**RELATED PROCEEDINGS APPENDIX**

None.